UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

STEPHANIE GAFFNEY, on Behalf of Herself and All Others Similarly Situated, Plaintiff, v. ONE BROOKLYN HEALTH SYSTEM, INC., Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Stephanie Gaffney ("Plaintiff") brings this Class Action Complaint on behalf of herself, and all others similarly situated, against Defendant One Brooklyn Health System, Inc. ("OBH" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to her, which are based on personal knowledge.

INTRODUCTION

1. Healthcare providers that handle sensitive, personally identifying information ("PII") or protected health information ("PHI") owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of PII or PHI to unauthorized persons – and especially hackers with nefarious intentions – will result in harm to the affected individuals, including, but not limited to, the invasion of their private health matters.

2. The harm resulting from a data and privacy breach manifests in a number of ways, including identity theft and financial fraud, and the exposure of a person's PII or PHI through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their

lives. Mitigating that risk – to the extent it is even possible to do so – requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and take a number of additional prophylactic measures.

3. As a healthcare provider, OBH knowingly obtains patient PII and PHI and has a resulting duty to securely maintain such information in confidence.

4. OBH's Notice of Privacy Practices states that it "values the privacy of each of its patients" and "is required by law to maintain confidentiality of [patients'] protected health information."[1]

5. Plaintiff brings this class action on behalf of individuals whose PII and/or PHI was accessed and exfiltrated by an unauthorized third party during a data breach of OBH's computer system, which Defendant discovered on or about November 19, 2022, but did not disclose until April 20, 2023 (the "Data Breach").[2]

6. Despite becoming aware of the Data Breach on or around November 19, 2022, OBH failed to timely notify Plaintiff and Class Members of the Data Breach within 60 days as required by law. Notably, Defendant failed to notify Plaintiff and Class Members for approximately 6 months after its discovery of the Data Breach.

7. Based on the public statements of OBH, a wide variety of PII and PHI was implicated in the Data Breach, including but not limited to, names, Social Security numbers, driver's license or state identification numbers, dates of birth, financial account information,

---

[1] *Notice of Privacy Practices*, ONE BROOKLYN HEALTH, https://onebrooklynhealth.org/media/abab33wi/obhs-notice-of-privacy-practices-04112023-4.docx (last visited May 8, 2023).

[2] *One Brooklyn Health Provides Notice of Data Security Incident*, ONE BROOKLYN HEALTH https://onebrooklynhealth.org/media/p4abqfwk/obh-website-notice.pdf (last visited May 8, 2023) ("Notice of Data Breach"); *One Brooklyn Health Reports Leaked Patient and Employee Information Following Recent Data Breach*, JDSUPRA (Apr. 24, 2023), https://www.jdsupra.com/legalnews/one-brooklyn-health-reports-leaked-3756261/ (last visited on May 8, 2023).

medical treatment information, prescription information, medical diagnosis or condition information, and health insurance information.[3]

8. As a direct and proximate result of Defendant's inadequate data security, and its breach of its duty to handle PII and PHI with reasonable care, Plaintiff's and Class Members' PII and PHI has been accessed by hackers and exposed to an untold number of unauthorized individuals.

9. Plaintiff, on behalf of herself and the Class as defined herein, brings claims for negligence, negligence *per se*, breach of implied contract, unjust enrichment, bailment, and declaratory judgment, seeking actual and putative damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief. Plaintiff and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of their health privacy, and similar forms of criminal mischief, risk which may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

10. To recover from Defendant for these harms, Plaintiff and the Class seek damages in an amount to be determined at trial, declaratory judgment, and injunctive relief requiring Defendant to: 1) disclose, expeditiously, the full nature of the Data Breach and the types of PII and PHI accessed, obtained, or exposed by the hackers; 2) implement improved data security practices to reasonably guard against future breaches of PII and PHI possessed by Defendant; and 3) provide, at its own expense, all impacted victims with lifetime identity theft protection services.

---

[3] Notice of Data Breach, *supra* note 2.

PARTIES

11. Plaintiff Stephanie Gaffney is an adult, who at all relevant times, is a resident and citizen of the State of New York. Plaintiff has been a patient of OBH's during the relevant period. In order to receive healthcare services, Plaintiff was required to entrust OBH with her PII and PHI, and in return reasonably expected that Defendant would implement adequate data security measures to safeguard her sensitive personal information. Plaintiff received a Data Breach notification informing her that the PII and PHI she provided to OBH had been compromised in the Data Breach.

12. Since receiving a Data Breach notification, Plaintiff has been required to expend her valuable time and resources communicating with the credit bureaus to place a freeze on her credit in order to prevent any misuses of her PII and PHI – time she would not have had to expend but for the Data Breach.

13. Since receiving a Data Breach notification Plaintiff has also received a significant increase in spam calls as compared to prior to the Data Breach. Plaintiff has also suffered emotional distress as a result of her PII and PHI being accessed and exposed to an unauthorized third-party.

14. As a result of the Data Breach, Plaintiff will continue to be at heightened and certainly impending risk for fraud and identity theft, and their attendant damages for years to come.

15. Defendant OBH is a New York not-for-profit corporation with a principal place of business located at 1 Brookdale Plaza, Brooklyn, New York 11212.

JURISDICTION AND VENUE

16. This Court has jurisdiction over this action pursuant to 28 U.S.C. §1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members

of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

17. This Court has personal jurisdiction over Defendant because Defendant resides in this District, and at all relevant times it has engaged in substantial business activities in New York.

18. Pursuant to 28 U.S.C. §1391(b)(1) and (2), venue is proper in this District because it is where the Defendant resides and is where a substantial part of the events or omissions giving rise to the claims occurred.

FACTUAL BACKGROUND

A. OBH and the Services it Provides

19. OBH is a Brooklyn-based healthcare company that operates three major hospitals and their affiliates in the surrounding area, including Brookdale Hospital Medical Center, Interfaith Medical Center, and Kingsbrook Jewish Medical Center.[4] OBH also operates a network of primary, behavior health, and specialty care locations, providing patients with a broad range of healthcare services, including pediatric and geriatric care, behavior health services, sickle cell services, podiatry, and maternal health services.[5]

20. While administering these healthcare services, OBH receives, handles, and collects sensitive patient PII and PHI, which includes, *inter alia*, names, Social Security numbers, driver's license or state identification numbers, dates of birth, financial account information, medical treatment information, prescription information, medical diagnosis or condition information, and health insurance information.

---

4 *About OBH*, ONE BROOKLYN HEALTH, https://onebrooklynhealth.org/about-us, (last visited May 8, 2023).

5 *Id*.

21. In order to receive these healthcare services, Plaintiff and Class Members are required to entrust their highly sensitive PII and PHI to OBH. Plaintiff and Class Members entrust this information to Defendant with the reasonable expectation and mutual understanding that OBH will comply with its obligations to keep such information confidential and secure from unauthorized access.

22. By obtaining, collecting, and storing Plaintiff's and Class Members' PII and PHI, OBH assumed legal and equitable duties and knew, or should have known, that it was responsible for protecting Plaintiff's and Class Members PII and PHI from unauthorized access.

23. Despite OBH stating that it "prioritizes its responsibility to safeguard the information it collects in providing services,"[6] Defendant nevertheless employed inadequate data security measures to protect and secure the PII and PHI patients entrusted to it, resulting in the Data Breach and the compromise of Plaintiff's and Class Members PII and PHI.

B. OBH Knew the Risks of Storing Valuable PII and PHI and the Foreseeable Harm to Victims

24. OBH was well aware that the PHI and PII it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

25. OBH also knew that a breach of its computer systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII and PHI was compromised, as well as intrusion into their highly private health information.

26. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at business such as Equifax, Facebook, Yahoo, Marriott, Anthem, and many others.

---

6 Notice of Data Breach, *supra* note 2.

27. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[7] PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

28. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2021, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[8]

29. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[9]

30. The healthcare industry has become a prime target for threat actors: "[h]igh demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[10]

---

[7] Brian Krebs, *The Value of a Hacked Company*, KREBS ON SEC. (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/ (last visited on May 8, 2023).

[8] *Data Breach Report: 2021 Year End*, RISK BASED SEC. (Feb. 4, 2022), https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/ (last visited on May 8, 2023).

[9] *Facts + Statistics: Identity theft and cybercrime,* INS. INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited May 8, 2023).

[10] *The healthcare industry is at risk*, SWIVELSECURE, https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited May 8, 2023).

31. Additionally, "[h]ospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily – making the industry a growing target."[11]

32. Cybercriminals seek out PHI at a greater rate than other sources of personal information. Between 2009 and 2022, 5,150 healthcare data breaches of 500 or more individuals have been reported to Health and Human Services' Office of Civil Rights, resulting in the exposure or unauthorized disclosure of the information of 382,262,109 individuals – "[t]hat equates to more than 1.2x the population of the United States."[12]

33. Further, the rate of healthcare data breaches has been on the rise in recent years. "In 2018, healthcare data breaches of 500 or more records were being reported at a rate of around 1 per day. Fast forward 5 years and the rate has more than doubled. In 2022, an average of 1.94 healthcare data breaches of 500 or more records were reported each day."[13]

34. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[14]

35. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July 2022. The percentage of

---

11 *Id.*

12 *Healthcare Data Breach Statistics*, HIPAA J., https://www.hipaajournal.com/healthcare-data-breach-statistics/, (last visited May 8, 2023).

13 *Id*.

14 *2022 Breach Barometer*, PROTENUS, https://www.protenus.com/breach-barometer-report (last visited May 8, 2023).

healthcare breaches attributed to malicious activity rose more than five percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[15]

36. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves OBH's patients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

37. **Social Security Numbers** – Unlike credit or debit card numbers in a payment card data breach – which can quickly be frozen and reissued in the aftermath of a breach – unique social security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

38. The Social Security Administration even warns that the process of replacing a Social Security is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with

[15] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, CYBERSECURITY NEWS (July 19, 2022), https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year (last visited on May 8, 2023).

> your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[16]

39. Social security numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit – among other services. Often social security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes social security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

40. **Driver's License Numbers** – are highly sought after by cyber criminals on the dark web because they are unique to a specific individual and extremely sensitive. This is because a Driver's License number is connected to an individual's vehicle registration, insurance policies, records on file with the DMV, places of employment, doctor's offices, government agencies, and other entities.

41. For these reasons, Driver's License numbers are highly sought out by cyber criminals because they are one of the most valuable pieces of information to facilitate identity theft and fraud. This information is valuable because cyber criminals can use this information to open credit card accounts, obtain insurance policies and submit fraudulent claims, open cell phone contracts, file fraudulent tax returns, file unemployment applications, as well as obtain bank loans under a person's name.

42. Further, unlike credit or debit card numbers in a payment card data breach, which can quickly be frozen and reissued in the aftermath of a breach, the type of PII at stake here – unique Driver's License numbers – cannot be easily replaced.

---

[16] *Identify Theft and Your Social Security Numbers*, SOCIAL SEC. ADMIN. (July 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited on May 8, 2023).

43. **Healthcare Records** – As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals – they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. 'Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to – we've even seen $60 or $70.'"[17] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[18]

44. Indeed, medical records "are so valuable because they can be used to commit a multitude of crimes. Healthcare data can be used to impersonate patients to obtain expensive medical services, Medicare and Medicaid benefits, healthcare devices, and prescription medications. Healthcare records also contain the necessary information to allow fraudulent tax returns to be filed to obtain rebates."[19]

45. "In contrast to credit card numbers and other financial information, healthcare data has an incredibly long lifespan and can often be misused for long periods undetected. Credit card companies monitor for fraud and rapidly block cards and accounts if suspicious activity is detected, but misuse of healthcare data is harder to identify and can be misused in many ways before any

---

17 *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data*, *New Ponemon Study Shows*, IDX (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat (last visited on May 8, 2023).

18 *Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security® Survey 2015*, PRICEWATERHOUSECOOPERS (Sept. 30, 2014), https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last visited May 8, 2023).

19 Steve Adler, *Editorial: Why Do Criminals Targer Medical Records*, HIPAA J. (Oct. 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records/#:~:text=Healthcare%20records%20are%20so%20valuable,credit%20cards%20in%20victims'%20names. (last visited on May 8, 2023).

malicious activity is detected. During that time, criminals can run up huge debts – far more than is usually possible with stolen credit card information."[20]

46. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[21]

47. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that

---

20 *Id*.

21 Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN (Mar. 31, 2023), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last visited on May 8, 2023).

attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[22]

48. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII and PHI about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

49. Based on the value of its patients' PII and PHI to cybercriminals, OBH knew or should have known, the importance of safeguarding the PII and PHI entrusted to it and of the foreseeable consequences if its data security systems were breached. OBH failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

C. OBH Breached Is Duty to Protect Its Patients' PII and PHI

50. On or about November 25, 2022, news outlets began reporting that OBH was suffering disruptions to its computer network systems, which led Defendant to take its computer systems offline on or about November 19, 2022.[23]

---

22 U.S. Gov't Accountability Off., GAO-07-737, Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown (2007), https://www.gao.gov/new.items/d07737.pdf, (last visited May 2, 2023).

23 Claudia Irizarry Aponte, *One Brooklyn Health System Offline After Unexplained IT Issue*, THE CITY (Nov. 25, 2022), https://www.thecity.nyc/2022/11/25/23478350/one-brooklyn-health-system-offline-kingsbrook-brookdale-interfaith-hospitals (last visited on May 8, 2023).

51. The computer systems disruption left OBH's "medical staff unable to access patient medical records or to upload laboratory and test results to electronic patient portals"[24] forcing Defendant to "operate using paper charts for multiple weeks"[25] and causing delays and outages that forced Defendant's patients to have to seek medical treatment at other hospitals.[26]

52. In January 2023, OBH confirmed that the disruptions to its computer systems were in fact the result of a cyber-attack, during which patient information was exfiltrated from its computer systems.[27] Around the same time, OBH reported the Data Breach to the Department of Health and Human Services Office for Civil Rights ("HHS"), indicating that 500 individuals were impacted by the Data Breach.[28]

53. Following the disruptions to its computer systems, OBH engaged external specialist and commenced an investigation into the nature and scope of the incident – *i.e.*, the Data Breach.[29]

54. According to Defendant, the investigation revealed that an unauthorized third-party gained access to OBH's computer systems and acquired OBH data.[30] The unauthorized third-party had access to Defendant's computer systems from approximately July 9, 2022 to November 19,

---

24 *Id*.

25 Jill McKeon, *One Brooklyn Confirms Cyberattack, BlackCat Ransomware Claims Attack on NextGen*, HEALTH IT SEC. (Jan. 24, 2023), https://healthitsecurity.com/news/one-brooklyn-confirms-cyberattack-blackcat-ransomware-claims-nextgen-attack (last visited on May 8, 2023).

26 Carl Campanile, *Computer crash causes chaos at Brooklyn hospitals network with ties to Hochul*, N.Y. POST (Nov. 29, 2022), https://nypost.com/2022/11/29/it-network-crash-at-brooklyn-hospitals-with-ties-to-hochul/ (last visited on May 8, 2023).

27 Giles Bruce, *One Brooklyn Health Says Hacker Copied Patient Data in Cyberattack*, BECKER'S HEALTH IT (Jan. 24, 2023), https://www.beckershospitalreview.com/cybersecurity/one-brooklyn-health-says-hacker-copied-patient-data-in-cyberattack.html (last visited on May 8, 2023).

28 *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, U.S. DEP'T OF HEALTH & HUM. SERVS. OFF. FOR C.R., https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf, (last visited May 8, 2023).

29 Notice of Data Breach, *supra* note 2.

30 *Id*.

2022.[31] In other words, OBH's computer systems were compromised for approximately five months before Defendant ever identified the unauthorized access.

55. OBH completed review of the information impacted by the Data Breach on or about March 21, 2023, and confirmed that personal and medical information relating to its patients was compromised during the Data Breach.[32]

56. The patient PII and PHI compromised during the Data Breach includes names, Social Security numbers, driver's license or state identification numbers, dates of birth, financial account information, medical treatment information, prescription information, medical diagnosis or condition information, and health insurance information.[33]

57. Approximately six months after first discovering the Data Breach, OBH began notifying individuals impacted by the Data Breach on or about April 20, 2023.[34] On or about that same date, Plaintiff received a notification indicating that her PII and PHI may have been compromised during the Data Breach.

58. Like Plaintiff, the Class Members received similar notices informing them that their PII and/or PHI was exposed in the Data Breach.

59. While Defendant has not yet updated the size of the Data Breach on HHS's breach reporting portal, OBH's notification to the Office of the Maine Attorney General indicated that approximately 235,000 individuals were impacted by the Data Breach.[35]

---

31 *Id*.

32 *Id*.

33 *Id*.

34 JDSupra, *supra* note 2.

35 *Data Breach Notifications*, OFF. OF THE ME. ATTY. GEN., (Apr. 20, 2022), https://apps.web.maine.gov/online/aeviewer/ME/40/73e780c9-ea42-4b82-9d46-41bc962aceb5.shtml (last visited on May 8, 2023).

60. The Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures in order to protect its patients' PII and PHI.

D. OBH Is Obligated Under HIPAA to Safeguard Personal Information

61. OBH is required by the Health Insurance Portability and Accountability Act, 42 U.S.C. §1302d, *et seq*. ("HIPAA") to safeguard patient PHI.

62. OBH is an entity covered by HIPAA, which sets minimum federal standards for privacy and security of PHI.

63. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. §164.302

64. Under 45 C.F.R. §160.103, HIPAA defines "protected health information" or PHI as "individually identifiable health information" that is "transmitted by electronic media"; "[m]aintained in electronic media"; or "[t]ransmitted or maintained in any other form or medium."

65. Under 45 C.F.R. §160.103, HIPAA defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2)"[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and (3) either (a) "identifies the individual"; or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual."

66. HIPAA requires OBH to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against

reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 CFR §164.102, *et. seq*.

67. HIPAA's security rules also require a covered entity to report a data breach without unreasonable delay and in no case later than 60 calendar days from the discovery of the breach.[36]

68. While HIPAA permits healthcare providers to disclose PHI to third parties under certain circumstances, HIPAA does not permit healthcare providers to disclose PHI to cybercriminals nor did Plaintiff or the Class Members consent to the disclosure of their PHI to cybercriminals.

69. As such, OBH is required under HIPAA to maintain the strictest confidentiality of Plaintiff's and Class Members' PHI that it requires, receives, and collects, and Defendant is further required to maintain sufficient safeguards to protect that information from being accessed by unauthorized third parties.

70. Given the application of HIPAA to OBH, and that Plaintiff and Class Members entrusted their PHI to Defendant in order to receive medical treatment, Plaintiff and Class Members reasonably expected that Defendant would safeguard their highly sensitive information and keep their PHI confidential.

E. FTC Guidelines Prohibit OBH from Engaging in Unfair or Deceptive Acts or Practices

71. OBH is prohibited by the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §45, from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable

[36] Steve Adler, *What are the HIPAA Breach Notification Requirements*, HIPAA J. (Feb. 11, 2023), https://www.hipaajournal.com/hipaa-breach-notification-requirements (last visited on May 8, 2023).

and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

72. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[37]

73. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[38]

74. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[39]

75. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

---

37 *Start with Security – A Guide for Business*, U.S. FED. TRADE COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited on May 8, 2023).

38 *Protecting Personal Information: A Guide for Business*, U.S. FED. TRADE COMM'N (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited on May 8, 2023)..

39 *Id*.

76. OBH failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

77. OBH was at all times fully aware of its obligations to protect the PII and PHI of patients because of its position as a healthcare provider, which gave it direct access to reams of patient PII and PHI. Defendant was also aware of the significant repercussions that would result from its failure to do so.

F. Plaintiff and Class Members Suffered Damages

78. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff, and members of the Class, significant injuries and harm in several ways. Plaintiff and members of the Class must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

79. Once PII and PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's conduct. Further, the value of Plaintiff and Class Members' PII and PHI has been diminished by its exposure in the Data Breach.

80. As a result of Defendant's failures, Plaintiff and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their PHI. Indeed, Plaintiff has

already suffered from fraudulent activity, as someone has opened a bank account in her name following the Data Breach.

81. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud – this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[40]

82. With respect to health care breaches, another study found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[41]

83. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[42]

84. The reality is that cybercriminals seek nefarious outcomes from a data breach and "stolen health data can be used to carry out a variety of crimes."[43]

---

40 Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KNOWBE4 (Mar. 7, 2023), https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud, (last visited May 8, 2023).

41 Jessica David, *70% of Data Involved in Healthcare Breaches Increases Risk of Fraud*, HEALTH IT SEC. (Sept. 25, 2019), https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud (last visited May 8, 2023).

42 *Id*.

43 Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited on May 8, 2023).

85. Health information in particular is likely to be used in detrimental ways – by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[44]

86. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[45]

87. Plaintiff and Class Members are also at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its patients' PII and PHI.

88. Plaintiff and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to strangers.

CLASS ALLEGATIONS

89. Plaintiff brings this class action on behalf of herself, and all other individuals who are similarly situated, pursuant to Rule 23 of the Federal Rules of Civil Procedure.

90. Plaintiff seeks to represent a class of persons to be defined as follows:

> All individuals in the United States and its territories whose PII and/or PHI was compromised in the OBH Data Breach which was discovered on or about November 19, 2022 (the "Class").

---

44 *Id*.

45 *The Potential Damages and Consequences of Medical Identity theft and Healthcare Data Breaches*, EXPERIAN (Apr. 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf, (last visited May 8, 2023).

91. Excluded from the Class are Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

92. This proposed class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the class definition in an amended pleading or when she moves for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

93. **Numerosity:** Plaintiff is informed and believes, and thereon alleges, that there are at minimum, thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Defendant's records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes approximately 235,000 individuals.

94. **Commonality:** This action involved questions of law and fact common to the Class. Such common questions include but are not limited to:

a. Whether Defendant had a duty to protect the PII and PHI of Plaintiff and Class Members;

b. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' PII and PHI, and breached its duties thereby;

c. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct; and

d. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

95. **Typicality:** Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiff and members of the Class were all patients of Defendant, each having their PII and PHI exposed and/or accessed by an unauthorized third party.

96. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the members of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and has no interests antagonistic to the members of the Class. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class Members are substantially identical as explained above.

97. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, expense, and promote uniform decision-making.

98. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class.

If Defendant breached its duty to Plaintiff and Class Members, then Plaintiff and each Class member suffered damages by that conduct.

99. **Injunctive Relief:** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23(b)(2).

100. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class Members may be readily identified through Defendant's books and records.

FIRST CAUSE OF ACTION
NEGLIGENCE
(Plaintiff on Behalf of the Class)

101. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

102. Defendant owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

103. OBH's duty to use reasonable care arose from several sources, including but not limited to those described below.

104. OBH has a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By receiving, maintaining, and handling PII and PHI that is routinely targeted by criminals for unauthorized access, OBH was obligated to act with reasonable care to protect against these foreseeable threats.

105. OBH's duty also arose from Defendant's position as a healthcare provider. OBH holds itself out as a trusted provider of healthcare services, thereby assuming a duty to reasonably protect the information it obtains from its patients. Indeed, Defendant, who receives, maintains, collects, and handles PII and PHI from its patients, was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

106. OBH breached the duties owed to Plaintiff and Class Members and was thus negligent. Although the exact methodologies employed by the unauthorized third parties are unknown to Plaintiff at this time, on information and belief, Defendant breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its patients; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII or PHI.

107. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII and PHI would not have been compromised.

108. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class members.

109. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE
(Plaintiff on Behalf of the Class)

110. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

111. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendant for failing to use reasonable measures to protect PII and PHI. Various FTC publications and orders also form the basis of OBH's duty.

112. OBH violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI its obtained and stored and the foreseeable consequences of a data breach involving the PII and PHI its entrusted from its patients.

113. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

114. Plaintiff and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

115. OBH is an entity covered under the HIPAA, which sets minimum federal standards for privacy and security of PHI.

116. Pursuant to HIPAA, 42 U.S.C. §1302d, *et. seq.*, and its implementing regulations, Defendant had a duty to implement and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect Plaintiff's and the Class members' electronic PHI.

117. Specifically, HIPAA required Defendant to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 CFR §164.102, *et. seq*.

118. Defendant violated HIPAA by actively disclosing Plaintiff's and the Class Members' electronic PHI; by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PHI; and by failing to timely notify Plaintiff and Class Members of a breach of their PHI.

119. Plaintiff and the Class Members are patients within the class of persons HIPAA was intended to protect, as they are patients of OBH.

120. Defendant's violation of HIPAA constitutes negligence *per se*.

121. The harm that has occurred as a result of Defendant's conduct is the type of harm that the FTC Act and HIPAA were intended to guard against.

122. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class members.

123. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(Plaintiff on Behalf of the Class)

124. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

125. Plaintiff brings this claim individually and on behalf of the Class.

126. When Plaintiff and members of the Class provided their PII and PHI to OBH in exchange for healthcare services, they entered into implied contracts with Defendant, under which OBH agreed to take reasonable steps to protect Plaintiff's and Class Members' PII and PHI, comply with it statutory and common law duties to protect Plaintiff's and Class Members' PII and PHI, and to timely notify them in the event of a data breach.

127. OBH solicited and invited Plaintiff and Class Members to provide their PII and PHI as part of Defendant's provision of healthcare services. Plaintiff and Class Members accepted

Defendant's offers when they made and paid for purchases of Defendant's services and products and provided their PII and PHI to Defendant.

128. When entering into implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with its statutory and common law duties to adequately protect Plaintiff's and Class Members' PII and PHI and to timely notify them in the event of a data breach.

129. OBH's implied promise to safeguard patient PII and PHI is evidenced by, *e.g.*, the representations in Defendant's Notice of Privacy Practices set forth above.

130. Plaintiff and Class Members paid money to OBH in order to receive healthcare services. Plaintiff and Class Members reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. OBH failed to do so.

131. Plaintiff and Class Members would not have provided their PII and PHI to OBH had they known that Defendant would not safeguard their PII and PHI, as promised, or provide timely notice of a data breach.

132. Plaintiff and Class Members fully performed their obligations under their implied contracts with OBH.

133. OBH breached its implied contracts with Plaintiff and Class Members by failing to safeguard Plaintiff's and Class Members' PII and PHI and by failing to provide them with timely and accurate notice of the Data Breach.

134. The losses and damages Plaintiff and Class Members sustained, include, but are not limited to:

a. Theft of their PII and/or PHI;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII and PHI;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

135. As a direct and proximate result of OBH's breach of contract, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(Plaintiff on Behalf of the Class)

136. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

137. Plaintiff brings this claim individually and on behalf of the Class in the alternative to Plaintiff's Breach of Implied Contract claim.

138. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

139. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

140. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased healthcare services from Defendant and/or its agents and in so doing provided Defendant with their PII and PHI. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PII and PHI protected with adequate data security.

141. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII and PHI of Plaintiff and Class Members for business purposes.

142. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII and PHI. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

143. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by its common law and statutory duties.

144. Defendant failed to secure Plaintiff and Class Members' PII and PHI and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

145. Defendant acquired the PII and PHI through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

146. If Plaintiff and Class Members knew that Defendant had not reasonably secured their PII and PHI, they would not have agreed to provide their PII and PHI to Defendant.

147. Plaintiff and Class Members have no adequate remedy at law.

148. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered injuries, including, but not limited to:

a. Theft of their PII and/or PHI;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII and PHI;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches

so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

149. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered damages and will continue to suffer other forms of injury and/or harm.

150. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

FIFTH CAUSE OF ACTION
BAILMENT
(Plaintiff on Behalf of the Class)

151. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

152. Plaintiff and Class Members delivered and entrusted their PII and PHI to OBH for the sale purpose of receiving healthcare services from Defendant.

153. In delivering their PII and PHI to OBH, Plaintiff and Class Members intended and understood that Defendant would employ adequate data security measures to safeguard their sensitive personal information.

154. Defendant accepted possession of Plaintiff's and Class Members' PII and PHI. By accepting possession, Defendant understood that Plaintiff and Class Members reasonably expected

OBH to adequately safeguard their sensitive personal information. Accordingly, a bailment was established for the mutual benefit of the parties.

155. During the bailment, OBH owed a duty to Plaintiff and Class members to exercise reasonable care in protecting their PII and PHI.

156. Defendant breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and Class Members' PII and PHI, resulting in the unauthorized access and exfiltration of such information.

157. Defendant further breached its duty to safeguard Plaintiff's and Class Members' PII and PHI by failing to notify them in a timely manner that their PII and PHI in OBH's possession had been compromised and exfiltrated.

158. As a direct and proximate result of OBH's breach of its duty, Plaintiff and Class members suffered consequential damages that were reasonably foreseeable to Defendant, including but not limited to the damages set forth herein.

SIXTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(Plaintiff on Behalf of the Class)

159. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

160. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et. seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

161. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and PHI and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that

compromise their PII and PHI. Plaintiff alleges that OBH's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her PII and PHI and remains at imminent risk that further compromises of her PII and/or PHI will occur in the future.

162. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed a legal duty to secure patients' PII and PHI under the common law, Section 5 of the FTC Act, and HIPAA; and

b. Defendant breached and continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII and PHI.

163. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect patients' PII and PHI.

164. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at OBH. The risk of another such breach is real, immediate, and substantial. If another breach at OBH occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

165. The hardship to Plaintiff and Class Members if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

166. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at OBH, thus eliminating the additional injuries that would result to Plaintiff, Class Members, and patients whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all other similarly situated, prays for relief as follows:

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

B. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

C. For damages in an amount to be determined by the trier of fact;

D. For an order of restitution and all other forms of equitable monetary relief;

E. Declaratory and injunctive relief as described herein;

F. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

G. Awarding pre- and post-judgment interest on any amounts awarded; and

H. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: May 9, 2023

Respectfully submitted,

/s/ Joseph P. Guglielmo
Joseph P. Guglielmo (JG-2447)
Ethan Binder (5769823)
SCOTT+SCOTT ATTORNEYS AT LAW LLP
230 Park Avenue, 17th Floor

New York, NY 10169
Telephone: 212-223-6444
Facsimile: 212-223-6334
jguglielmo@scott-scott.com
ebinder@scott-scott.com

Gary F. Lynch (*pro hac vice* forthcoming)
Jamisen A. Etzel (*pro hac vice* forthcoming)
Nicholas A. Colella (*pro hac vice* forthcoming)
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
Facsimile: (412) 231-0246
gary@lcllp.com
jamisen@lcllp.com
nickc@lcllp.com

Attorneys for Plaintiff